REMARKS

Claims 1-34 are currently pending in the application. By this amendment, claims 1, 21 and 28 are amended for the Examiner's consideration. The foregoing separate sheets marked as "Listing of Claims" shows all the claims in the application, with an indication of the current status of each.

The Examiner's indication that claims 2, 3/20/2, 4-9/2, 12-14/2, and 18-20/2 are allowable is acknowledged with appreciation.

The Examiner has rejected claims 1-34 under 35 U.S.C. §112, second paragraph, on the ground that the negative limitation added in the previous amendment "without extracting or otherwise decoding information in said Encoded Data Array" is not supported in the specification. However, it will be observed that the specification refers to "flash correlation" technology which has the ability to compare images in such a manner as to determine whether a "flash correlation artifact" is present. For example, if the artifact is present upon comparison of a Resultant Image and an encrypted version of the Original Image, then the Resultant Image is authentic (page 2, lines 27-29). It is not necessary to decrypt the Resultant Image or to perform pixel by pixel comparison in order to authenticate the image" (page 2, line 29, to page 3, line 2).

Similarly, the Resultant Image may be compared to an encrypted representation of the Encoded Data Array, and if the artifact is present, then it is verified that the Encoded Data Array is embedded in the Resultant Image. Further, the individual values (date/time, location, source, etc) of the Encoded Data Array may be separately represented in an image and verified (page 2, lines 25-29). If the comparison (e.g. by "flash correlation") is performed on an encrypted or encoded representation, and verification is accomplished thereby, it is clear that the

determination does not require extracting or otherwise decoding the representation itself, which has been encoded and/or encrypted (see page 4, line 30, to page 5, line 2). All that is required is that, in fact, the underlying information was imbedded in the image to be compared. If that is true, then – in the implementation using "flash correlation" – an artifact will be present upon comparison.

This is a very powerful technique. As described above, each of the embedded elements of information (e.g. date/time, location, source, etc.) can be encoded in a separate image and separately compared, as well as using the combination of elements in the Encoded Data Array, all without decoding the information in the encoded image. Thus, each of the elements can be separately tested. As to each element, or any combination of elements, the question can be asked, "is this element or combination of elements embedded" in the image being tested (e.g. the "target composite array" in claims 21 and 28). This flexibility, combined with encryption, provides users of the invention with the ability to design the authentication process so that

> "Certain recipients may be given the ability to decrypt the Resultant Image but not the ability to decode the Encoded Data Array.
>
> "Other recipients may be given the ability to extract the Encoding, or to authenticate one or more of the camera ID, frame number, date/time, location, and user ID, but not the ability to extract and authenticate all of them" (page 8, lines 12-19)

Furthermore, this technology permits multiple sets of encoded layers to be authenticated, since each layer can be separately and independently validated:

> The work may have previously been encoded with other date, time, and source. Multiple sets of encoded layers may be applied without affecting the accuracy of the authentication. That ability to overlay and separately readout multiple layers is an important advantage of flash correlation. (Page 10, lines 11-17)

All this can be done using the information that has been encrypted and/or encoded into a two dimensional image, without decrypting or decoding the information itself. Thus the invention is able to apply the underlying technology (e.g. flash correlation as described in U.S. Patent No. 5,583,950 issued to the present inventor) in a novel manner to overcome limitations in the prior art of authenticating the validity and security of digital evidence.

The independent claims have been amended to more clearly claim the novel capabilities of the invention.

The Examiner has rejected claims 1, 4-5/1, 8-9/1, 12-14/1, 18-20/1, 22-24, and 28 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,799,082 to Murphy et al. ("Murphy") in view of U.S. Patent No. 5,646,977 to Barton and U.S. Patent No. 6,642,956 to Safai and further in view of U.S. Patent No. 5,349,550 to Gage. The remarks submitted in response filed on November 3, 2005, are incorporated by reference and are maintained except where inconsistent with the present remarks. It is noted that the Examiner responds to the claim amendment (characterized by the Examiner as "comparing without extracting or decoding information in the encoded data array") by citing the Gage reference. Gage provides a correlation scheme for measuring the correlation coefficient of arbitrarily long digital sequences, and says nothing about authentication, embedded images or triggers. From the passage cited by the Examiner (Gage: col. 1, lines 12-33), it would appear that the Examiner has constructed a paraphrase of the claim language (i.e. "comparing without extracting or decoding") that substantially changes the meaning of the actual claim language. The cited passage from Gage describes "the field of binary data correlation", where two bit streams are compared for common bits, adjusting the alignment to produce an optimum synchronization.

Gage appears to be entirely irrelevant to the plain meaning of the claim language. The reason "without extracting or otherwise decoding information" has meaning in the claim is that the point of the comparison is precisely to ascertain whether the subject "information" in one array (the Encoded Data Array) has been embedded in the other array (the Composite Array), without determining what the information itself is (i.e. "without extracting or other decoding" the information). The binary data correlation either 1) has no such information or 2) such information is the bit content itself, which is "in the clear". As described in Gage, it is the bit content itself that is being compared. There is no pretense of actually comparing information content that is "encoded" by means of the bit content. Any such "encoding" would be an assumption not supported by Gage itself. Furthermore, the data array of the present invention is "embedded" (claim 1, line 18; claim 21, line 16; claim 28, line 16). There is no corresponding concept in the Gage reference, which is a fatal defect since the clear language of the claim addresses the ability of the "comparing means" to determine whether an encoded array is "embedded" in a target array being tested.

In summary, the Gage reference fails to address all the elements in the stated claim language, and therefore fails as a reference. While it is proper to give claim language its broadest reasonable interpretation, it is not a reasonable interpretation to ignore language contained in the very claim element being interpreted. It cannot be sound practice, consistent with justiciable standards of claim interpretation, simply to argue that "Gage teaches comparing" (which is correct) and then assert that since Gage is silent about "extracting or otherwise decoding information in said encoded data array" it is therefore reasonable to interpret the term "without" as reading on Gage.

It is therefore submitted that the foregoing ground of rejection is overcome.

The Examiner has rejected claims 6/1, 10-11/1, 25-27, and 32-34 under 35 U.S.C. §103(a) as being unpatentable over Murphy and Barton, Safai and Gage as applied to claims 1, 21 and 28, and further in view of U.S. Patent No. 5,583,950 to Prokoski. The Examiner has rejected claim 3/20/1 under 35 U.S.C. §103(a) as being unpatentable over Murphy, Barton, Safai and Gage as applied to claim 1, and further in view of U.S. Patent No. 5,862,217 to Steinberg. The Examiner has rejected claim 7/1 under 35 U.S.C. §103(a) as being unpatentable over Murphy, Barton, Safai and Gage as applied to claim 1, and further in view of U.S. Patent No. 5,841,886 to Rhoads. The Examiner has rejected claims 15-17 under 35 U.S.C. §103(a) as being unpatentable over Murphy, Barton, Safai and Gage as applied to claim 1, and further in view of U.S. Patent No. 6,526,158 to Goldberg. Since these rejected claims depend from claims now believed to be in allowable form, it is believed that these further rejections are also overcome.

Several additional comments are appropriate regarding the Examiner's points on a number of the dependent claims:

With respect to claim 3, the cited passage from Steinberg refers to the steps shown in Fig. 3, where the process provides for an initial encryption of the image with a temporary encryptor (item 95), which is then decrypted (item 98) prior to a final encryption (item 104) of the image. Thus the temporary encryption is, in fact, temporary and does not persist. This does not disclose what is disclosed and claimed in the present invention, namely, that different successive composite images, each being created by the addition of authentication information, could be the subject of a further authentication step by recursive repetition of the steps of the invention. No such repetition is disclosed or suggested by Steinberg. The Examiner has argued that Steinberg teaches the steps performed twice (col. 5, lines 5-20). However, it will be observed – as already stated – that Steinberg's initial encryption is temporary and

does not persist. In particular, this initial encryption is decrypted (item 98 in Fig. 3), so that the second and final encryption does not operate upon the temporary encryption. This is contrast to the present invention, where each of the repetitive encryptions operates upon the encrypted image from the prior encryption, as described above with respect to "multiple sets of encoded layers" (page 10, lines 13-14). The claims have been amended to clarify this point.

With respect to claim 14, the cited passage from Murphy discloses that downloading of an image for authentication can be initiated ("triggered") by a hardware key device (col. 15, line 29). That is, an "authorized digital frame downloader" can use a hardware or software key to request and implement the download. While the Examiner has mentioned only the hardware key, because "change of status of another device" cannot read on "software key", it should be clear that the real "trigger" is the human being that is the "downloader". The distinction between "software key" and "hardware key" is unimportant, because either could be used by the downloader. However, the claim is addressed to a "change of status". It is difficult to argue that a downloader's use of a key (hardware or software) is a "change of status of a device" as contemplated by the claim. Indeed, the trigger is the "change of status", not the use of a device. Indeed, the "device" could be a system implemented by software, as indicated by the language of claim 15. It is submitted that the disclosure of Murphy does not read on "change of status of a device" but only reads on "triggered by ... [use of] a device". The Examiner has not given meaning to the language actually used in the claim, and has instead rewritten the claim language so that it means something different (and contrary to) the stated meaning. This goes beyond the "broadest reasonable interpretation" of the claim language.

Without the Murphy predicate, the grounds for rejection of claims 15-17 must also fall. The cited passages from Goldberg do not appear to disclose an independent

triggering of the camera but rather a coordination and analysis of the image. For example, there is no suggestion that an image is triggered by a face recognition device, but rather that the location of a patron's face in the image can be determined using feature recognition programs. This is clearly after the fact and has nothing to do with triggering the image capture. The images in Goldberg are taken by fixed cameras in an entertainment venue where the patrons carry an electronic identification tag that is decoded by readers positioned at various locations. Since there are many patrons, the issue is one of coordinating images with patron ID information sensed by the readers. However, it is clear that image capture is not triggered by these readers but rather, for example, by an amusement ride car passing a switch (item 143 in Fig. 3). The Examiner argues that the triggering

In any event, claims 14-17 depend from claim 1, and since claim 1 is now believed to be in allowable form those claims depending from claim 1 are also allowable.

With respect to claims 26-27 and 33-34, Murphy's disclosure does not permit what is claimed, that is, a single processing step for authenticating the entire stack of sequential images. While it is true that the present inventor's prior patent (Prokoski '950) contemplates processing a stack of images, one skilled in the art would not be able to apply this teaching to Murphy, whose disclosure requires a separate examination of each image for authentication purposes. Murphy would have to be modified in accordance with the present invention, which is impermissible hindsight. But in any event, these claims depend from claims now believed to be in allowable form and therefore are also allowable.

In view of the foregoing, it is requested that the application be reconsidered, that claims 1-34 be allowed, and that the application be passed to issue.